

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2001-176189
(P2001-176189A)

(43) 公開日 平成13年6月29日 (2001.6.29)

(51) Int.Cl. ⁷	識別記号	F I	テーマート* (参考)
G 1 1 B 20/10		G 1 1 B 20/10	H 5 D 0 4 4
G 0 9 C 1/00	6 6 0	G 0 9 C 1/00	6 6 0 D 5 J 1 0 4

審査請求 未請求 請求項の数16 O L (全 16 頁)

(21) 出願番号 特願平11-354991

(22) 出願日 平成11年12月14日 (1999. 12. 14)

(71) 出願人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番35号

(72) 発明者 大澤 義知

東京都品川区北品川6丁目7番35号 ソニ
ー株式会社内

(72) 発明者 浅野 智之

東京都品川区北品川6丁目7番35号 ソニ
ー株式会社内

(74) 代理人 100067736

弁理士 小池 晃 (外2名)

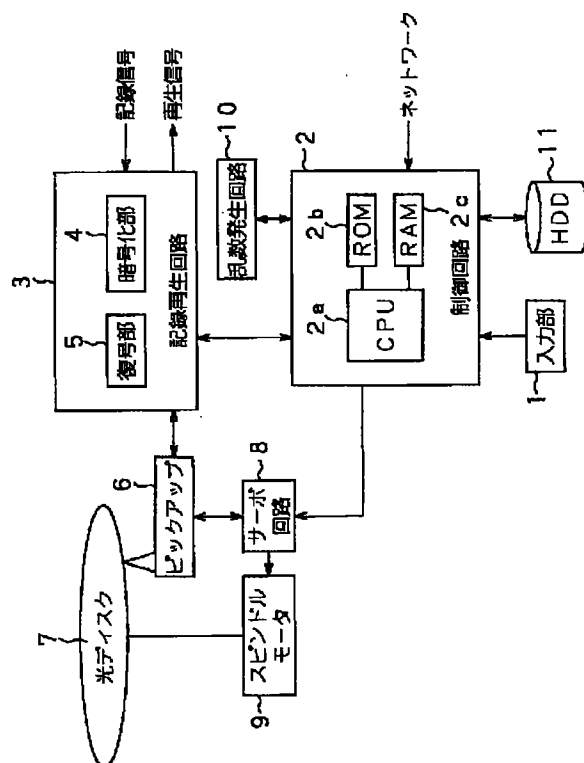
最終頁に続く

(54) 【発明の名称】 記録装置及び方法、再生装置及び方法並びに記録媒体

(57) 【要約】

【課題】 不正コピーを防止する。

【解決手段】 着脱可能な光ディスク7に情報を記録及び／又は再生する光ディスク記録再生装置であって、記録再生回路3において光ディスク7から第1の識別情報であるディスク製造識別情報DiscIDr及び第2の識別情報であるディスク記録識別情報DiscIDmを読み出すが、光ディスク7にディスク記録識別情報DiscIDrが記録されておらずディスク記録識別情報DiscIDrが得られないと、制御回路2は、乱数発生回路10で発生された乱数を光ディスク7にディスク記録識別情報DiscIDrとして書き込むように制御する。



【特許請求の範囲】

【請求項 1】 着脱可能な記録媒体に情報を記録する記録装置において、

記録媒体から第 1 の識別情報を読み出す第 1 の読み出し手段と、

上記記録媒体から第 2 の識別情報を読み出す第 2 の読み出し手段と、

数列を発生する数列発生手段と、

上記数列発生手段で発生された数列を上記記録媒体に第 2 の識別情報として書き込む書き込み手段とを有し、

上記記録媒体に第 2 の識別情報が記録されておらず上記第 2 の読み出し手段による読み出しにより第 2 の識別情報が得られないとき、上記書き込み手段により第 2 の識別情報を書き込みことを特徴とする記録装置。

【請求項 2】 上記数列発生手段は、疑似乱数、時刻情報又は処理の累積度数に基づいたビット列を発生することを特徴とする請求項 1 記載の記録装置。

【請求項 3】 着脱可能な記録媒体に情報を記録する記録装置において、

記録媒体から第 1 の識別情報を読み出す第 1 の読み出し手段と、

上記記録媒体から第 2 の識別情報を読み出す第 2 の読み出し手段と、

第 1 の秘密情報を格納する格納手段と、

上記第 1 の識別情報、上記第 2 の識別情報及び上記第 1 の秘密情報に基づいて第 2 の秘密情報を算出する第 2 の秘密情報算出手段と、

上記第 2 の秘密情報を用いて情報を暗号化し、上記記録媒体に記録する第 1 の暗号化書き込み手段とを有することを特徴とする記録装置。

【請求項 4】 第 3 の秘密情報を発生する第 3 の秘密情報発生手段と、上記第 3 の秘密情報を用いて情報を暗号化し、上記記録媒体に記録する第 2 の暗号化書き込み手段と、上記第 2 の秘密情報を用いて上記第 3 の秘密情報を暗号化し、上記記録媒体に記録する第 3 の暗号化書き込み手段とを有することを特徴とする請求項 3 記載の記録装置。

【請求項 5】 上記秘密情報発生手段は、疑似乱数に基づいたビット列を発生することを特徴とする請求項 3 記載の記録装置。

【請求項 6】 着脱可能な記録媒体に情報を記録する記録方法において、

記録媒体から第 1 の識別情報を読み出す第 1 の読み出し工程と、

上記記録媒体から第 2 の識別情報を読み出す第 2 の読み出し工程と、

数列を発生する数列発生工程と、

上記数列発生工程で発生された数列を上記記録媒体に第 2 の識別情報として書き込む書き込み工程とを有し、

上記記録媒体に第 2 の識別情報が記録されておらず上記

第 2 の読み出し工程による読み出しにより第 2 の識別情報が得られないとき、上記書き込み工程により第 2 の識別情報を書き込むことを特徴とする記録方法。

【請求項 7】 着脱可能な記録媒体に情報を記録する記録方法において、

記録媒体から第 1 の識別情報を読み出す第 1 の読み出し工程と、

上記記録媒体から第 2 の識別情報を読み出す第 2 の読み出し工程と、

10 上記第 1 の識別情報、上記第 2 の識別情報及び格納された第 1 の秘密情報に基づいて第 2 の秘密情報を算出する第 2 の秘密情報算出工程と、

上記第 2 の秘密情報を用いて情報を暗号化し、上記記録媒体に記録する第 1 の暗号化書き込み工程とを有することを特徴とする記録方法。

【請求項 8】 第 3 の秘密情報を発生する秘密情報発生工程と、上記第 3 の秘密情報を用いて情報を暗号化し、上記記録媒体に記録する第 2 の暗号化書き込み手段と、上記第 2 の秘密情報を用いて上記第 3 の秘密情報を暗号化し、上記記録媒体に記録する第 3 の暗号化書き込み手段とを有することを特徴とする請求項 7 記載の記録方法。

【請求項 9】 着脱可能な記録媒体から情報を再生する再生装置において、

記録媒体から第 1 の識別情報を読み出す第 1 の読み出し手段と、

上記記録媒体から第 2 の識別情報を読み出す第 2 の読み出し手段と、

第 1 の秘密情報を格納する格納手段と、

30 上記第 1 の識別情報、上記第 2 の識別情報及び上記第 1 の秘密情報に基づいて第 2 の秘密情報を算出する第 2 の秘密情報算出手段と、

上記記録媒体から暗号化された情報を読み出し、この情報を上記第 2 の秘密情報を用いて復号する第 1 の読み出し復号手段とを有することを特徴とする再生装置。

【請求項 10】 上記記録媒体から暗号化された第 3 の秘密情報を読み出す第 3 の読み出し手段と、上記第 2 の秘密情報を用いて暗号化された第 3 の秘密情報を復号する第 3 の秘密情報復号手段と、上記記録媒体から暗号化された情報を読み出し、この情報を上記第 3 の秘密情報を用いて復号する第 2 の読み出し復号手段とを有することを特徴とする請求項 9 記載の再生装置。

【請求項 11】 着脱可能な記録媒体から情報を再生する再生方法において、

記録媒体から第 1 の識別情報を読み出す第 1 の読み出し工程と、

上記記録媒体から第 2 の識別情報を読み出す第 2 の読み出し工程と、

上記第 1 の識別情報、上記第 2 の識別情報及び格納された第 1 の秘密情報に基づいて第 2 の秘密情報を算出する第 2 の秘密情報算出工程と、

上記記録媒体から暗号化された情報を読み出し、この情報を上記第2の秘密情報を用いて復号する第1の読み出し復号工程とを有することを特徴とする再生方法。

【請求項12】 上記記録媒体から暗号化された第3の秘密情報を読み出す第3の読み出し工程と、上記第2の秘密情報を用いて暗号化された第3の秘密情報を復号する第3の秘密情報復号工程と、上記記録媒体から暗号化された情報を読み出し、この情報を上記第3の秘密情報を用いて復号する第2の読み出し復号工程とを有することを特徴とする請求項1記載の再生方法。

【請求項13】 情報が記録される記録媒体において、所定の領域に第1の識別情報が記録され、第2の情報が記録される領域を有し、上記第1の識別情報及び第2の識別情報に基づいて算出された秘密情報を用いて暗号化された情報が書き込まれ、読み出された暗号化された情報を、上記秘密情報を用いて復号されることを特徴とする記録媒体。

【請求項14】 情報を記録媒体に記録するプログラムが記録された記録媒体において、上記プログラムは、記録媒体から第1の識別情報を読み出す第1の読み出し工程と、上記記録媒体から第2の識別情報を読み出す第2の読み出し工程と、数列を発生する数列発生工程と、上記数列発生工程で発生された数列を上記記録媒体に第2の識別情報として書き込む書き込み工程とを有し、上記記録媒体に第2の識別情報が記録されておらず上記第2の読み出し工程による読み出しにより第2の識別情報が得られないとき、上記書き込み工程により第2の識別情報を書き込むことを特徴とする記録媒体。

【請求項15】 情報を記録媒体に記録するプログラムが記録された記録媒体において、上記プログラムは、記録媒体から第1の識別情報を読み出す第1の読み出し工程と、上記記録媒体から第2の識別情報を読み出す第2の読み出し工程と、第1の秘密情報を格納する格納手段と、上記第1の識別情報、上記第2の識別情報及び上記第1の秘密情報に基づいて第2の秘密情報を算出する第2の秘密情報算出工程と、上記第2の秘密情報を用いて情報を暗号化し、上記記録媒体に記録する第1の暗号化書き込み工程とを有することを特徴とする記録媒体。

【請求項16】 情報を記録媒体から再生するプログラムが記録された記録媒体において、上記プログラムは、記録媒体から第1の識別情報を読み出す第1の読み出し手段と、上記記録媒体から第2の識別情報を読み出す第2の読み出し手段と、

第1の秘密情報を格納する格納手段と、

上記第1の識別情報、上記第2の識別情報及び上記第1の秘密情報に基づいて第2の秘密情報を算出する第2の秘密情報算出手段と、

上記記録媒体から暗号化された情報を読み出し、この情報を上記第2の秘密情報を用いて復号する第1の読み出し復号手段とを有することを特徴とする記録媒体。

【発明の詳細な説明】

【0001】

10 【発明の属する技術分野】本発明は、記録媒体に情報信号を記録する記録装置及び方法、記録媒体から情報信号を再生する再生装置及び方法並びに情報信号を記録される記録媒体に関する。

【0002】

【従来の技術】近年、情報をデジタル的に記録する記録機器および記録媒体が普及しつつある。これらの記録機器および記録媒体は、例えば、映像や音楽のデータを劣化させることなく記録し、再生するので、データを、その質を維持しながら何度もコピーすることができる。しかしながら、映像や音楽のデータの著作権者にしてみれば、自らが著作権を有するデータが、その質を維持しながら何度も不正にコピーされ、市場に流通してしまう恐れがある。このため、記録機器および記録媒体の側で、著作権を有するデータが不正にコピーされるのを防ぐ必要がある。

【0003】例えば、ミニディスク(MD)(商標)システムにおいては、シリアルコピー管理システム(Serial Copy Management System; SCMS)と呼ばれる方法が用いられている。これは、デジタルインタフェースによって、音楽データとともに伝送される情報のことである。この情報は、音楽データが、コピー自由(copy free)、コピー一度許容(copy once allowed)、またはコピー禁止(copy prohibited)のうちのいずれのデータであるのかを表す。ミニディスクレコーダは、デジタルインタフェースから音楽データを受信した場合、SCMSを検出し、これが、copy prohibitedであれば、音楽データをミニディスクに記録せず、copy once allowedであれば、これをcopy prohibitedに変更し、受信した音楽データとともに記録し、copy freeであれば、これをそのまま、受信した音楽データとともに記録する。

【0004】このようにして、ミニディスクシステムにおいては、SCMSを用いて、著作権を有するデータが不正にコピーされるのを防いでいる。

【0005】また、著作権を有するデータが不正にコピーされるのを防ぐ別の例としては、Digital Versatile Disk(DVD)(商標)システムにおける、コンテンツスクランブルシステムがあげられる。このシステムでは、ディスク上の、著作権を有するデータが全て暗号化され、ライセンスを受けた記録機器だけが暗号鍵を与えられ、これにより暗号化されたデータを復号し、意味のあるデ

ータを得ることができるようになされている。そして、記録機器は、ライセンスを受ける際に、不正コピーを行わない等の動作規定に従うように設計される。このようにして、DVDシステムにおいては、著作権を有するデータが不正にコピーされるのを防いでいる。

【0006】

【発明が解決しようとする課題】上記のミニディスクシステムが採用している方式では、SCMSがcopy once allowedであれば、これをcopy prohibitedに変更し、受信したデータとともに記録することが規定されている。しかし、このような動作規定に従わない記録機器が、不正に製造されてしまう。

【0007】また、上記のDVDシステムが採用している方式は、ROMメディアに対しては有効であるが、ユーザがデータを記録可能なRAMメディアにおいては有効ではない。RAMメディアにおいては、不正者は、暗号を解読できない場合であっても、ディスク上のデータを全部、新しいディスクに不正にコピーすることによって、ライセンスを受けた正当な記録機器で動作するディスクを新たに作ることができるからである。

【0008】本発明は、上述の実情に鑑みてなされたものであり、記録媒体に不正コピーを抑制するように記録する記録装置及び方法、記録媒体からの不正コピーを抑制するように再生する再生装置及び方法並びに不正コピーを抑制するような記録媒体に関する。

【0009】

【課題を解決するための手段】上述の課題を解決するために、本発明に係る記録装置は、着脱可能な記録媒体に情報を記録する記録装置において、記録媒体から第1の識別情報を読み出す第1の読み出し手段と、上記記録媒体から第2の識別情報を読み出す第2の読み出し手段と、数列を発生する数列発生手段と、上記数列発生手段で発生された数列を上記記録媒体に第2の識別情報として書き込む書き込み手段とを有し、上記記録媒体に第2の識別情報が記録されておらず上記第2の読み出し手段による読み出しにより第2の識別情報が得られないとき、上記書き込み手段により第2の識別情報を書き込むものである。

【0010】また、本発明に係る記録装置は、着脱可能な記録媒体に情報を記録する記録装置において、記録媒体から第1の識別情報を読み出す第1の読み出し手段と、上記記録媒体から第2の識別情報を読み出す第2の読み出し手段と、第1の秘密情報を格納する格納手段と、上記第1の識別情報、上記第2の識別情報及び上記第1の秘密情報に基づいて第2の秘密情報を算出する第2の秘密情報算出手段と、上記第2の秘密情報を用いて情報を暗号化し、上記記録媒体に記録する第1の暗号化書き込み手段とを有するものである。

【0011】本発明に係る記録方法は、着脱可能な記録媒体に情報を記録する記録方法において、記録媒体から

第1の識別情報を読み出す第1の読み出し工程と、上記記録媒体から第2の識別情報を読み出す第2の読み出し工程と、数列を発生する数列発生工程と、上記数列発生工程で発生された数列を上記記録媒体に第2の識別情報として書き込む書き込み工程とを有し、上記記録媒体に第2の識別情報が記録されておらず上記第2の読み出し工程による読み出しにより第2の識別情報が得られないとき、上記書き込み工程により第2の識別情報を書き込むものである。

10 【0012】また、本発明に係る記録方法は、着脱可能な記録媒体に情報を記録する記録方法において、記録媒体から第1の識別情報を読み出す第1の読み出し工程と、上記記録媒体から第2の識別情報を読み出す第2の読み出し工程と、上記第1の識別情報、上記第2の識別情報及び格納された第1の秘密情報に基づいて第2の秘密情報を算出する第2の秘密情報算出工程と、上記第2の秘密情報を用いて情報を暗号化し、上記記録媒体に記録する第1の暗号化書き込み工程とを有するものである。

20 【0013】本発明に係る再生装置は、着脱可能な記録媒体から情報を再生する再生装置において、記録媒体から第1の識別情報を読み出す第1の読み出し手段と、上記記録媒体から第2の識別情報を読み出す第2の読み出し手段と、第1の秘密情報を格納する格納手段と、上記第1の識別情報、上記第2の識別情報及び上記第1の秘密情報に基づいて第2の秘密情報を算出する第2の秘密情報算出手段と、上記記録媒体から暗号化された情報を読み出し、この情報を上記第2の秘密情報を用いて復号する第1の読み出し復号手段とを有するものである。

30 【0014】本発明に係る再生方法は、着脱可能な記録媒体から情報を再生する再生方法において、記録媒体から第1の識別情報を読み出す第1の読み出し工程と、上記記録媒体から第2の識別情報を読み出す第2の読み出し工程と、上記第1の識別情報、上記第2の識別情報及び格納された第1の秘密情報に基づいて第2の秘密情報を算出する第2の秘密情報算出工程と、上記記録媒体から暗号化された情報を読み出し、この情報を上記第2の秘密情報を用いて復号する第1の読み出し復号工程とを有するものである。

40 【0015】本発明に係る記録媒体は、情報が記録される記録媒体において、所定の領域に第1の識別情報が記録され、第2の情報が記録される領域を有し、上記第1の識別情報及び第2の識別情報に基づいて算出された秘密情報を用いて暗号化された情報が書き込まれ、読み出された暗号化された情報を、上記秘密情報を用いて復号されるものである。

50 【0016】また、本発明に係る記録媒体は、情報を記録媒体に記録するプログラムが記録された記録媒体において、上記プログラムは、記録媒体から第1の識別情報を読み出す第1の読み出し工程と、上記記録媒体から第

2の識別情報を読み出す第2の読み出し工程と、数列を発生する数列発生工程と、上記数列発生工程で発生された数列を上記記録媒体に第2の識別情報として書き込む書き込み工程とを有し、上記記録媒体に第2の識別情報が記録されておらず上記第2の読み出し工程による読み出しにより第2の識別情報が得られないとき、上記書き込み工程により第2の識別情報を書き込むものである。

【0017】さらに、本発明に係る記録媒体は、情報を記録媒体に記録するプログラムが記録された記録媒体において、上記プログラムは、記録媒体から第1の識別情報を読み出す第1の読み出し工程と、上記記録媒体から第2の識別情報を読み出す第2の読み出し工程と、第1の秘密情報を格納する格納手段と、上記第1の識別情報、上記第2の識別情報及び上記第1の秘密情報に基づいて第2の秘密情報を算出する第2の秘密情報算出工程と、上記第2の秘密情報を用いて情報を暗号化し、上記記録媒体に記録する第1の暗号化書き込み工程とを有するものである。

【0018】そして、本発明に係る記録媒体は、情報を記録媒体から再生するプログラムが記録された記録媒体において、上記プログラムは、記録媒体から第1の識別情報を読み出す第1の読み出し手段と、上記記録媒体から第2の識別情報を読み出す第2の読み出し手段と、第1の秘密情報を格納する格納手段と、上記第1の識別情報、上記第2の識別情報及び上記第1の秘密情報に基づいて第2の秘密情報を算出する第2の秘密情報算出手段と、上記記録媒体から暗号化された情報を読み出し、この情報を上記第2の秘密情報を用いて復号する第1の読み出し復号手段とを有するものである。

【0019】本発明は、第3の秘密情報を発生し、上記第3の秘密情報を用いて情報を暗号化して上記記録媒体に書き込み、上記第2の秘密情報を上記第2の秘密情報を暗号化して上記記録媒体に書き込むものである。この第3の秘密情報とは、上記第1の秘密情報及び第2の秘密情報の下位にある秘密情報を意味するものである。

【0020】

【発明の実施の形態】以下では、本発明の実施の形態について、図面を参照して説明する。まず、本発明の実施の形態として、光ディスク記録再生装置について説明する。

【0021】図1は、光ディスク記録再生装置の構成例を表している。入力部1は、ボタン、スイッチ、リモートコントローラなどにより構成され、ユーザにより入力操作されたとき、その入力操作に対応する信号を出力する。

【0022】制御回路2は、プログラムに従って処理を実行するCPU2a、不揮発性の記憶素子であるROM2b、揮発性の記憶素子であるRAM2cなどにより構成されている。この制御回路2は、ROM2bやRAM2cに記憶された所定のプログラムに従って、装置全体

を制御する。

【0023】制御回路2は、ROM2bに格納されたプログラムで動作する。制御回路2には、外部のネットワークや、HDD11からプログラムが読み込まれる可能性がある。例えば、制御回路2にパーソナルコンピュータを用い、読み込んだコンピュータプログラムに用いて処理を実行させることができる。

【0024】記録再生回路3は、暗号化部4と復号部5を有し、復号部5は、ピックアップ6により、光ディスク7から再生されたデータを復号し、外部に再生信号として出力する。暗号化部4は、外部から記録信号の供給を受け取ると、これを暗号化し、ピックアップ6に供給して、光ディスク7に記録させる。

【0025】ピックアップ6は、レーザビームを光ディスク7に照射することで、データの記録再生を行う。スピンドルモータ9は、サーボ回路8によって制御され、光ディスク7を回転させる。

【0026】サーボ回路8は、スピンドルモータ9を駆動することにより、光ディスク7を所定の速度、例えば線速度一定で回転させる。サーボ回路8はまた、ピックアップ6のトラッキングおよびフォーカシングの他、スレッドサーボを制御する。

【0027】乱数発生回路10は、制御回路2の制御により、所定の乱数を発生する。HDD11は、プログラムやデータを記録される大容量の記録装置である。

【0028】ここで、本実施の形態の前提となる、特願平10-025310号明細書に記載されている記録方法について説明する。この記録方法によると、光ディスク7には、図2に示すような構造を有するデータが記録される。

【0029】光ディスク7のリードインエリアには、製造者により光ディスク7に付与された第1の識別情報であるディスク製造識別情報DiscIDmを予め暗号化した暗号化ディスク製造識別情報EDiscIDm、ディスクキーKdを暗号化した暗号化ディスクキーEKdが記録されている。なお、上記ではDiscIDmを暗号化しているが、この暗号化とは、実際はそのアクセス方法を知らない者には読み出し、書き込みが困難なように記録することで、便宜上これを暗号化と呼んでいる。

【0030】この記録方法によると、個々の光ディスク7を識別するためのディスク製造識別情報DiscIDmを光ディスク7に持たせ、この情報をライセンスを受けた装置にしかアクセスできないようにする。

【0031】また、光ディスク7のデータエリアには、ヘッダである暗号化セクタキーEKs1とメインデータ部である暗号化コンテンツデータとからなるセクタS1が記録されている。暗号化セクタキーEKs1はディスクキーKdにより、暗号化コンテンツデータはセクタキーKs1により、それぞれ暗号化されている。なお、図中の括弧は暗号化に用いる秘密情報を示している。

【0032】同様に、光ディスク7のデータエリアには、ヘッダである暗号化セクタキーEKs2とメインデータ部である暗号化コンテンツデータとからなるセクタS2が記録されている。暗号化セクタキーEKs2はディスクキーKdにより、暗号化コンテンツデータはセクタキーKs2により、それぞれ暗号化されている。

【0033】光ディスク7上のデータはディスク製造識別情報DiscIDmと、ライセンスを受けることによって得られる秘密情報、例えば秘密鍵によって暗号化し、ライセンスを受けていない装置はデータを読み出しても意味のないものとする。装置にライセンスを与える際にはその動作を規定し、不正コピーを行わないようにする。

【0034】ライセンスを得ていない装置はディスク製造識別情報DiscIDmにアクセスできず、またディスク製造識別情報DiscIDmは個々の光ディスク7ごとに個別の値になっているため、ライセンスを受けていない機器がアクセス可能なすべての情報を新たな光ディスク7にコピーしたとしても、そのようにして作られた光ディスク7は、ライセンスを受けていない装置でもライセンスを受けた装置でも正しく情報が読み出せないようにしている。このようにして不正コピーを防いでいる。

【0035】この記録方法では、ディスク製造識別情報DiscIDmを光ディスク7の製造時に製造者が記録する、という運用方法と、ある媒体に初めてデータを記録する記録装置がこの際に媒体識別情報を媒体に記録するという運用方法がある。

【0036】ところで、前者の方法では下記のような問題がある。

【0037】ディスク製造識別情報DiscIDmは光ディスク7ごとに固有の値でなければならないが、そうすることは製造者によってコストの増加を招くため、すべての光ディスク7に同一の値を記録するような製造者が出る可能性がある。

【0038】また、すべての光ディスク7に同一のディスク製造識別情報DiscIDmが記録されてしまうと、ライセンスを受けていない装置はその情報がアクセスできないとしても、装置間で同一なので、アクセスできる情報だけコピーすれば、まったく同じ光ディスク7ができてしまい、不正コピーが可能になってしまう。

【0039】また、後者の方法では下記のような問題がある。ディスク製造識別情報DiscIDmは、ライセンスを受けていない装置はアクセスできないようにしなければならないため、そのアクセス方法はライセンスを受けた装置だけが持つ秘密情報となる。

【0040】さらに、前者の方法においては、ディスク製造識別情報DiscIDmの記録方法は光ディスク7の製造者のみが知っていればよいが、この方法においては、すべての記録装置がディスク製造識別情報DiscIDmの記録方法を持つことが必要である。

【0041】このことは、不正なコピーを試みる攻撃者

にとって、前者の方法よりも、ディスク製造識別情報DiscIDmの記録方法を盗み出す機会が容易に手に入るということになる。このため、この方法においては、不正者がディスク製造識別情報DiscIDmにアクセスする可能性が高く、セキュリティが低くなるという問題がある。

【0042】本実施の形態では、このような問題を解決するために、識別情報の記録方法として、製造者が記録する第1の識別情報と、記録装置が記録する第2の識別情報の両方を用いる。

【0043】上記の2つの識別情報を用いることにより、たとえ製造者が同一の第1の識別情報を記録した光ディスク7を複数製造しても、記録装置がそれぞれ別個の第2の識別情報を記録するので、識別情報全体として別個のものとなり、識別情報にアクセスされない限り不正コピーを防ぐことが可能となる。

【0044】また、たとえ記録機器が持つ第2の識別情報の記録方法を不正者が盗んだとしても、それだけでは製造者が記録した第1の識別情報にアクセスすることはできず、この場合も不正コピーを防ぐことが可能となる。

【0045】本実施の形態においては、光ディスク7には、図3に示すような構造を有するデータが記録されている。光ディスク7のリードインエリアには、ディスク製造識別情報DiscIDmを第1の秘密情報である予め定められたM系列符号で暗号化した暗号化ディスク製造識別情報EDiscIDm、ディスクキーKdをイフェクティブマスタキーKemで暗号化した暗号化ディスクキーEKdが記録されている。

【0046】また、光ディスク7には、光ディスク記録再生装置により、第2の識別情報であるディスク記録識別情報DiscIDrが付与される。このディスク記録識別情報DiscIDrは、M系列符号にて暗号化された暗号化ディスク記録識別情報EDiscIDrとして光ディスク7に記録される。光ディスク7には、暗号化ディスク記録識別情報EDiscIDrを記録するための領域が予め設けられている。

【0047】このように、ディスク製造識別情報DiscIDm及びディスク記録識別情報DiscIDrを暗号化していることにより、これらの識別情報に対する不正なアクセスを阻止することができる。すなわち、識別情報の暗号化は、ライセンスを受けていない者やライセンスを受けていない機器が、上記識別情報を読んだり、書きかえたり、新規に書いたりことを防止する。なお、この暗号化は、必ずしも数学的な意味での暗号化でなくても、その方法を知らない者が読み出し、書き込み等のアクセスを行うのが困難という程度のものでもよい。

【0048】暗号化ディスク製造識別情報EDiscIDm及び暗号化ディスク記録識別情報EDiscIDrは、光ディスクの読み出し専用のROM部分や、書き換え可能なRAM部分や、ROM部分やRAM部分に組み合わせて書くことができる。本実施の形態における記録方式については、

後述する。

【0049】上記M系列符号は、所定の周期で、“0”と“1”の2値がランダムに出現する疑似ランダム2値信号、すなわち一種の疑似乱数である。ディスク製造識別情報DiscIDmは、例えば、ファイル名やディレクトリ情報などのTOC(Table Of Contents)データ内に、予め設定された所定のM系列符号に基づいて埋め込むことで暗号化されている。すなわち、ディスク製造識別情報DiscIDmは、TOCデータのエッジの時間ずれとして記録される。このような暗号化を行うと、TOCデータは暗号化されないでM系列符号がなくとも読み取ることができるが、ディスク製造識別情報DiscIDmは、暗号化に用いたのと同じM系列符号がないと読み取ること、すなわち復号することができなくなる。このようなM系列符号に基づく暗号化に関する技術は、特願平09-288960号として本出願人が先に提案している。なお、この所定のM系列符号は、著作権者から適正なライセンスを受ける際、後述する第2の秘密情報であるマスターキーKmとともに、ライセンスを受けた者に与えられる。

【0050】上記イフェクティブマスターキーKemは、式(1)に従い、マスターキーKm、ディスク製造識別情報DiscIDm、ディスク記録識別情報DiscIDrに基づいて、ハッシュ(hash)関数を適用することにより計算される。

【0051】

$$Kem = SHA-1(Km || DiscIDm || DiscIDr) \quad (1)$$

ここで、“Km||DiscIDm||DiscIDr”は、マスターキーKm、DiscIDm、DiscIDrのビット連結を表している。例えば、AとBとCの連結とは、それぞれが n_A 、 n_B 、 n_C ビットであるとき、Aの後方にBを、Bの後方にCを結合して $n_A + n_B + n_C$ ビットのデータとすることを意味し、これを“A||B||C”で表すものとする。

【0052】また、SHA-1は、“Federal Information Processing Standards Publication(FIPS) 180-1”に定義されている一方向ハッシュ関数である。SHA-1の出力は、160ビットであるが、実際にはイフェクティブマスターキーKemは最上位から必要なビット数だけ取り出すなどして使用する。

【0053】マスターキーKmは、著作権者等から適正にライセンスを受けた光ディスク記録再生装置にだけ与えられる秘密情報である。

【0054】光ディスク7のデータエリアの各セクタSi($i=1,2,\dots$)は、ヘッダおよびメインデータ部で構成され、ヘッダには、セクタキーKsiをディスクキーKdで暗号化した暗号化セクタキーEKsi($i=1,2,\dots$)が格納されている。ここでKsiのiは、セクタの番号を示し、セクタキーはセクタ毎に異なるのでKsiと記述するが、特に区別する必要がない場合は、Ksとも記述する。メインデータ部には、コンテンツデータをセクタキーKsiで暗号化した暗号化コンテンツデータが格納されている。

【0055】図4は、暗号化部4の構成例を表してい

る。

【0056】DiscID暗号化復号回路21は、DiscIDm復号回路21a、DiscIDr暗号化復号回路21bから構成されている。

【0057】DiscIDm復号回路21aは、光ディスク7から読み出された暗号化ディスク製造識別情報EDiscIDmを、M系列符号発生回路22から供給された、暗号化に用いたのと同じM系列符号に基づいて復号し、ディスク製造識別情報DiscIDmを再現する。

【0058】ディスク記録識別情報DiscIDr暗号化復号回路21bは、光ディスク7から読み出された暗号化ディスク記録識別情報EDiscIDrを、M系列符号発生回路22から供給される、暗号化に用いたのと同じM系列符号に基づいて復号し、ディスク記録識別情報DiscIDrを再現する。識別情報DiscID暗号化復号回路21はまた、乱数発生回路10から発生された乱数をディスク記録識別情報DiscIDrとして受け取り、M系列符号発生回路22から供給されるM系列符号に基づいて暗号化して、ディスク記録識別情報EDiscIDrを生成し、光ディスク7に記録する。

【0059】M系列符号発生回路22は、例えば、直列接続された複数のフリップフロップとイクスクルーシブオア回路からなり、所定のM系列符号を発生するようになされている。あるいは、ROM、EEPROMなどで構成することもできる。

【0060】連結回路29は、DiscIDm復号回路21aにて復号されたディスク製造識別情報DiscIDm、DiscIDr暗号化復号回路21bにて復号されたディスク記録識別情報DiscIDrを連結し、識別情報DiscIDを生成する。

【0061】Kem発生モジュール23のKmメモリ24は、マスターキーKmを記憶する。Kem発生モジュール23のhash関数回路25は、マスターキーKmと識別情報DiscIDの結合を生成し、これにハッシュ(hash)関数を適用してイフェクティブマスターキーKemを算出する。

【0062】Kd暗号化復号回路26は、光ディスク7から読み出された暗号化ディスクキーEKdを、イフェクティブマスターキーKemで復号して、ディスクキーKdを再現する。Kd暗号化復号回路26はまた、乱数発生回路10から発生された乱数をディスクキーKdとして受け取り、イフェクティブマスターキーKemで暗号化して暗号化ディスクキーEKdを生成し、光ディスク7に記録する。

【0063】例えば、この暗号化方式としては、“Federal Information Processing Standards (FIPS) 46-2”に示されているデータ暗号化標準(Data Encryption Standard; DES)などが挙げられる。なお、Ks暗号化回路27及びコンテンツデータ暗号化回路28においても同様である。

【0064】Ks暗号化回路27は、乱数発生回路10から発生された乱数をセクタキーKsとして受け取り、ディスクキーKdで暗号化して暗号化セクタキーEKsを生成

し、光ディスク 7 に記録する。コンテンツデータ暗号化回路 28 は、セクタキー Ks で、コンテンツデータを暗号化し、光ディスク 7 に記録する。全データの記録が終了するまでコンテンツデータの暗号化、記録を繰り返す。

【0065】ここで、コンテンツデータの暗号化鍵にイフエクティブマスタキー Kem そのものを使う方法もあるが、一回の記録を表すファイルや、光ディスク 7 への読み書きの最小単位であるセクタ毎に、コンテンツデータを直接暗号化するセクタキー Ks のようなコンテンツキーを設け、それをイフエクティブマスタキー Kem で暗号化して、コンテンツデータと同様に光ディスク 7 に記録するなど、鍵を階層化して使用する方法も一般的である。なお、コンテンツキーは、セクタキー Ks に限られず、例えばファイルキーであってもよい。

【0066】次に、図 5 に、復号部 5 の構成例を示す。EDiscID 復号回路 51 は、EDiscIDm 復号回路 51a、EDiscIDr 復号回路 51b から構成されている。

【0067】EDiscIDm 復号回路 51a は、光ディスク 7 から読み出された暗号化ディスク製造識別情報 EDiscIDm を、M 系列符号発生回路 52 から供給される、暗号化に用いたのと同じ M 系列符号に基づいて復号して、ディスク製造識別情報 DiscIDm を再現する。

【0068】EDiscIDr 復号回路 51b は、光ディスク 7 から読み出された暗号化ディスク記録識別情報 EDiscIDr を、M 系列符号発生回路 52 から供給される、暗号化に用いたのと同じ M 系列符号に基づいて復号して、ディスク記録識別情報 DiscIDr を再現する。

【0069】M 系列符号発生回路 52 は、M 系列符号発生回路 22 と同様の構成を有し、同一の M 系列符号を発生するようになっている。

【0070】連結回路 59 は、DiscIDm 復号回路 51a にて復号されたディスク製造識別情報 DiscIDm、ディスク記録識別情報 DiscIDr 暗号化復号回路 51b にて復号されたディスク記録識別情報 DiscIDr を連結し、識別情報 DiscID を生成する。この連結回路 59 は、連結回路 29 と同様の構成を有し、同様の連結処理を行うようになっている。

【0071】Kem 発生モジュール 53 の Km メモリ 54 は、マスタキー Km を記憶する。Kem 発生モジュール 53 の hash 関数回路 55 は、マスタキー Km と識別情報 DiscID の結合を生成し、これにハッシュ (hash) 関数を適用してイフエクティブマスタキー Kem を計算する。この Kem 発生モジュール 53 は、Kem 発生モジュール 23 と同一の構成とされ、両者を兼用するようにしてもよい。

【0072】EKd 復号回路 56 は、光ディスク 7 から読み出された暗号化ディスクキー EKd を、イフエクティブマスタキー Kem で復号して、ディスクキー Kd を算出する。EKs 復号回路 57 は、光ディスク 7 から各セクタ Si のヘッダに記録されている暗号化セクタキー EKs を読み出し、ディスクキー Kd で復号して、セクタキー Ks を算出

する。コンテンツデータ復号回路 58 は、光ディスク 7 から読み出された暗号化されたコンテンツデータを、セクタキー Ks で復号する。

【0073】光ディスク記録再生装置において用いられる光ディスク 7 は、製造時にディスク製造識別情報 DiscIDm が書き込まれている。この光ディスク 7 は、ディスク製造識別情報 DiscIDm が書き込まれた状態で、ユーザで光ディスク 7 の製造者から提供される。

【0074】図 6 は、光ディスク 7 にディスク製造識別情報 DiscIDm を書き込む DiscIDm 書き込み装置 60 の構成例を示す。

【0075】この書き込み処理は、通常は光ディスク 7 の製造者により行われる。この光ディスク 7 には、ディスク記録識別情報 DiscIDr を記録するための領域を設けておく。

【0076】乱数回路 61 は、64 ビットの乱数を生成する。M 系列符号発生回路 62 は、M 系列符号発生回路 22 と同様の構成を有し、M 系列符号発生回路 62 と同一の M 系列符号を発生するようになっている。

【0077】DiscIDm 暗号化回路 63 は、乱数発生回路 61 で生成された乱数をディスク製造識別情報 DiscIDm として受け取り、M 系列符号発生回路 62 から供給される M 系列符号に基づいて、上述したように、入力される TOC 情報に埋め込むように暗号化して、暗号化ディスク製造識別情報 EDiscIDm を生成し、光ディスク 7 に記録する。

【0078】次に、光ディスク 7 の製造時に、ディスク製造識別情報 DiscIDm 書き込み装置により光ディスク 7 にディスク製造識別情報 DiscIDm を書き込む処理手順を、図 7 のフローチャートを参照して説明する。

【0079】最初に、ステップ S31 において、乱数発生回路 61 は、64 ビットの乱数を発生し、ディスク製造識別情報 DiscIDm として、DiscIDm 暗号化回路 63 に出力する。

【0080】ディスク製造識別情報 DiscIDm は、個々の光ディスク 7 について個別の値を使用する。たとえば、個別に割り振られた製造者の識別番号と、その製造者が製造したこの光ディスク 7 の累積度数すなわちシリアル番号を連結したものをディスク製造識別情報 DiscIDm とする。

【0081】なお、ディスク製造識別情報 DiscIDm は完全にユニークである必要はない。これは、ディスク製造識別情報 DiscIDm が同一である複数の光ディスク 7 が不正者の手に入らなければよいので、ディスク製造識別情報 DiscIDm が同一である複数の光ディスク 7 を探し出すのが困難であるようになっていればよいからである。このため、本実施の形態では、ディスク製造識別情報 DiscIDm の生成にその場で発生させた擬似乱数を用いている。なお、時刻情報などを用いることも可能である。

【0082】光ディスク 7 への記録は、ライセンスを受

けた機器のみがディスク製造識別情報DiscIDmを読み出せるように、ライセンスによる秘密情報に基づいた方法により行われる。すなわち、ステップS32において、DiscIDm暗号化回路63は、乱数発生回路61から供給されたディスク製造識別情報DiscIDmを、M系列符号発生回路62から供給されたM系列符号に基づいて、上述したように、TOC情報中に埋め込むようにして暗号化して、暗号化ディスク製造識別情報EDiscIDmを生成する。M系列符号は、ライセンスにより与えられるものである。

【0083】そして、ステップS33において、暗号化ディスク製造識別情報EDiscIDmを光ディスク7のリードインエリアに記録する。また、後にディスク製造識別情報DiscIDmを書きかえられないように、光ディスク7に設けた一度しか記録できないライトワンス領域にディスク製造識別情報DiscIDmを記録することも有効である。

【0084】次に、光ディスク7に対して、ユーザデータを記録する場合の暗号化部4における処理手順を、図8のフローチャートを参照して説明する。

【0085】最初に、ステップS50Aにおいて、DiscIDm復号回路21aは、光ディスク7のリードインエリアから読み出された暗号化ディスク製造識別情報EDiscIDmを受け取る。

【0086】ステップS50Bにおいて、DiscIDm暗号化復号回路21aは、この光ディスク7から読み出された暗号化ディスク製造識別情報EDiscIDmを、M系列符号発生回路22から供給された、暗号化に用いたのと同じM系列符号で復号して、ディスク製造識別情報DiscIDmとする。このように、ライセンスされた秘密情報を用いて、光ディスク7からディスク製造識別情報DiscIDmが得られた。

【0087】ステップS50Cにおいて、DiscIDr暗号化復号回路21は、光ディスク7のリードインエリアから読み出された暗号化ディスク記録識別情報EDiscIDrを受け取り、またKd暗号化復号回路26は、光ディスク7のリードインエリアから読み出された暗号化ディスクキーEKdを受け取る。

【0088】次に、ステップS51において、DiscIDr暗号化復号回路21は、光ディスク7のリードインエリアに、暗号化ディスク記録識別情報EDiscIDrが書き込まれているか否か、すなわち暗号化ディスク記録識別情報EDiscIDrを受けることができたか否かの判定を行い、Kd暗号化復号回路26は、光ディスク7のリードインエリアに、暗号化ディスクキーEKdが書き込まれているか否か、すなわち暗号化ディスクキーEKdを受け取ることができたか否かの判定を行う。暗号化ディスク記録識別情報EDiscIDrと暗号化ディスクキーEKdが共に書き込まれていないと判定された場合、ステップS52に進み、乱数発生回路10は、64ビットの乱数を発生し、ディスク記録識別情報DiscIDrとして、DiscIDr暗号化復号回路

21に出力する。

【0089】この乱数は、ディスク記録識別情報DiscIDrとして個々の光ディスク7について個別の値を使用するために用いられる。なお、乱数に限らず、たとえば、個別に割り振られた記録再生装置の識別番号と、その記録再生が生成したディスク記録識別情報DiscIDrの個数を連結したものをディスク記録識別情報DiscIDrとしてもよい。

【0090】ディスク記録識別情報DiscIDrは完全にユニークである必要はない。これは、ディスク記録識別情報DiscIDrが同一である複数の光ディスク7が不正者の手に入らなければよいので、ディスク記録識別情報DiscIDrが同一である複数の光ディスク7を探し出すのが困難であるようになっていけばよい。

【0091】このため、ディスク記録識別情報DiscIDrの生成にその場で発生させた擬似乱数を用いている。なお、時刻情報などを用いることも可能である。

【0092】ステップS53において、連結部29は、DiscIDm復号回路21aにて復号されたディスク製造識別情報DiscIDmと、乱数発生回路10からDiscIDr暗号化復号回路21bに送られたディスク記録識別情報DiscIDrとを連結し、識別情報DiscIDを生成する。

【0093】次に、ステップS54において、DiscIDr暗号化復号回路21bは、乱数発生回路10から供給されたディスク記録識別情報DiscIDrを、M系列符号発生回路22から供給されたM系列符号に基づいて暗号化して、暗号化ディスク記録識別情報EDiscIDrを生成し、光ディスク7に記録する。

【0094】また、後にディスク記録識別情報DiscIDrを書きかえられないように、光ディスク7に設けた一度しか情報を記録できないライトワンス領域にディスク記録識別情報DiscIDrを記録することも有効である。

【0095】このステップでは、光ディスク7にディスク記録識別情報DiscIDrが記録されていないので、光ディスク記録再生装置はその光ディスク7用のディスク記録識別情報DiscIDrを生成し、ライセンスされた秘密情報を用いてこれを光ディスク7に記録する。

【0096】この、光ディスク7への記録は、ライセンスを受けた機器のみがディスク記録識別情報DiscIDrを読み出せるように、ライセンス秘密情報に基づいた方法により行われる。

【0097】次に、ステップS55において、Kem発生モジュール23のhash関数回路25は、Kem発生モジュール23のKmメモリ24から、ライセンスされた秘密情報として与えられ、秘密に保管しているマスタキーKmを読み出す。Kem発生モジュール23のhash関数回路25は、ステップS56で、上述の式(1)に従い、光ディスク7の識別情報DiscID、およびKmメモリ24から読み出したマスタキーKmの結合にhash関数を適用して、イフェクティブマスタキーKemを計算し、Kd暗号化復号回路

26に供給する。

【0098】次に、ステップS57において、乱数発生回路10は、40ビットの乱数を発生し、ディスクキーKdとして、Kd暗号化復号回路26に出力する。Kd暗号化復号回路26は、ステップS58において、乱数発生回路10から供給されたディスクキーKdを、hash関数回路25から受け取ったイフェクティブマスタキーKemにより暗号化して、暗号化ディスクキーEKdを生成し、光ディスク7のリードインエリアに記録する。

【0099】ステップS52で、暗号化ディスク記録識別情報EDiscIDrと暗号化ディスクキーEKdが書き込まれていると判定された場合、ステップS59Aに進み、DiscIDr暗号化復号回路21bは、この光ディスク7から読み出された暗号化ディスク記録識別情報EDiscIDrを、M系列符号回路22から供給された、暗号化に用いたのと同じM系列符号で復号して、ディスク記録識別情報DiscIDrとする。このように、ライセンスされた秘密情報を用いて、ディスク記録識別情報DiscIDrが得られた。

【0100】ステップS59Bにおいて、連結部29は、DiscIDm復号回路21aにて復号されたディスク製造識別情報DiscIDmと、DiscIDr暗号化復号回路21bにて復号されたディスク記録識別情報DiscIDrとを連結し、識別情報DiscIDを生成する。

【0101】ステップS60において、Kem発生モジュール23のhash関数回路25は、Kem発生モジュール23のKmメモリ24から、マスタキーKmを読み出す。Kem発生モジュール23のhash関数回路25は、ステップS61で、上述の式(1)に従い、光ディスク7の識別情報DiscIDとマスタキーKmの結合にhash関数を適用して、イフェクティブマスタキーKemを計算し、Kd暗号化復号回路26に供給する。

【0102】次に、ステップS62において、Kd暗号化復号回路26は、この光ディスク7から読み出された暗号化ディスクキーEKdを、hash関数回路25から受け取ったイフェクティブマスタキーKemで復号して、ディスクキーKdを得る。Kd暗号化復号回路26は、ディスクキーKdを、Ks暗号化回路27に出力する。

【0103】ステップS58またはS62の処理の後、乱数発生回路10は、ステップS63で、40ビットの乱数を発生し、セクタキーKsとして、Ks暗号化回路27、およびコンテンツデータ暗号化回路28に出力する。Ks暗号化回路27は、ステップS64で、暗号化ディスクキーEKdが光ディスク7に記録されている場合にはKd暗号化復号回路26、または暗号化ディスクキーEKdが光ディスク7に記録されていない場合には乱数発生回路10から受け取ったディスクキーKdで、乱数発生回路10から受け取ったセクタキーKsを暗号化して、暗号化セクタキーEKsを生成する。Ks暗号化回路27はまた、その暗号化セクタキーEKsを、光ディスク7のデー

タエリアにあるセクタヘッダに記録する。

【0104】次に、ステップS65において、コンテンツデータ暗号化回路28は、ステップS63で乱数発生回路10から受け取ったセクタキーKsにより、コンテンツデータを暗号化し、光ディスク7のデータエリアのメインデータ部に記録する。

【0105】ステップS66において、暗号化部4の各回路は、全てのコンテンツデータを記録したか否かの判定を行う。全てのコンテンツデータがまだ記録されていないと判定された場合、ステップS67に進み、暗号化部4の各回路は、光ディスク7の、まだデータを記録していないセクタにアクセスし、ステップS63に戻り、以下同様の処理を繰り返す。ステップS66で、全てのコンテンツデータが記録されたと判定された場合、暗号化部4の各回路は、全ての記録処理を終了する。

【0106】以上のようにして、ディスク記録識別情報DiscIDrが生成され、記録媒体に記録され、そして生成されたディスク記録識別情報DiscIDrとマスタキーKmに対応して暗号化されたコンテンツデータが記録媒体に記録される。このことより、例えば、ディスク製造識別情報DiscIDmは記録されているがディスク記録識別情報DiscIDrは記録されていない既存の記録媒体に複製されたコンテンツデータを、著作権者から適正にライセンスを受けていない者は、意味のある情報として再生することができない。

【0107】次に、図9のフローチャートを参照して、復号部5により行われる、ユーザデータの再生処理を説明する。

【0108】最初に、ステップS81Aにおいて、EDiscIDm復号回路51aは、光ディスク7のリードインエリアから読み出された、暗号化されたディスク製造識別情報DiscIDmである暗号化識別情報EDiscIDmを受け取る。ステップS81Bにおいて、EDiscIDr復号回路51bは、光ディスク7のリードインエリアから読み出された、暗号化されたディスク記録識別情報DiscIDrである暗号化ディスク記録識別情報EDiscIDrを受け取る。

【0109】EDiscIDm復号回路51aはさらに、ステップS82Aにおいて、M系列符号発生回路52から供給されたM系列符号に基づいて、暗号化ディスク製造識別情報EDiscIDmを復号してディスク製造識別情報DiscIDmを再現し、連結回路59に出力する。

【0110】EDiscIDr復号回路51bはさらに、ステップS82Bにおいて、M系列符号発生回路52から供給されたM系列符号に基づいて、暗号化ディスク記録識別情報EDiscIDrを復号してディスク記録識別情報DiscIDrを再現し、連結回路59に出力する。

【0111】このように、ライセンスによる秘密情報として与えられた方法を用いて、光ディスク7からディスク製造識別情報DiscIDmとディスク記録識別情報DiscIDrが得られた。

【0112】ステップS82Cにおいて、連結回路59は、EDiscID復号回路51aで復号されたディスク製造識別情報DiscIDmと、EDiscIDr復号回路51bで復号されたディスク記録識別情報DiscIDrとを連結し、識別情報DiscIDとする。

【0113】次に、ステップS83において、Km発生モジュール53のhash関数回路55は、連結回路59から出力された識別情報DiscIDを受け取るとともに、Kmメモリ54からライセンスによる秘密情報として与えられ、秘密に保管しているマスタキーKmを読み出し、上述の式(1)に従い、光ディスク7の識別情報DiscIDとマスタキーKmの結合にhash関数を適用してイフェクティブマスタキーKemを算出し、EKd復号回路56に供給する。

【0114】ステップS84において、EKd復号回路56は、光ディスク7のリードインエリアから読み出された暗号化ディスクキーEKdを受け取る。EKd復号回路56は、ステップS85で、この読み出された暗号化ディスクキーEKdを、hash関数回路55から受け取ったイフェクティブマスタキーKemで復号して、ディスクキーKdを算出し、EKs復号回路57に出力する。

【0115】次に、ステップS86において、EKs復号回路57は、光ディスク7のデータエリアから読み出された各セクタの暗号化セクタキーEKsi (i=1,2,...)を受け取る。EKs復号回路57は、ステップS87で、この読み出された暗号化セクタキーEKsiを、EKd復号回路56から受け取ったディスクキーKdで復号して、セクタキーKsiを算出し、コンテンツデータ復号回路58に出力する。

【0116】ステップS88において、コンテンツデータ復号回路58は、光ディスク7から読み出された暗号化されているコンテンツデータを受け取る。コンテンツデータ復号回路58は、ステップS89で、この読み出された暗号化されているコンテンツデータを、EKs復号回路57から受け取ったセクタキーKsiで復号し、再生信号として出力する。

【0117】次に、ステップS90において、復号部5の各回路は、光ディスク7のデータエリアから、全てのコンテンツデータを読み出したか否かの判定を行う。全てのコンテンツデータがまだ読み出されていないと判定された場合、ステップS91に進み、復号部5の各回路は、光ディスク7の、まだ読み出されていない次のセクタのデータの供給を受け、ステップS86以降の処理を繰り返す。全てのコンテンツデータが読み出されたと判定された場合、復号部5の各回路は、全ての再生処理を終了する。

【0118】このように、記録媒体のIDを生成し、所定のM系列符号で暗号化して、記録媒体に記録することで、著作権者から適正にライセンスを受けた者だけが、その記録媒体にアクセスできるようにする。

【0119】なお、本実施の形態中において、上記処理

を実行するコンピュータプログラムをユーザに提供する提供媒体には、磁気ディスク、CD-ROMなどの情報記録媒体の他、インターネット、デジタル衛星などのネットワークによる伝送媒体も含まれる。

【0120】また、本発明は、光ディスク以外の記録媒体にデータを記録または再生する場合にも適用が可能である。

【0121】さらに、本実施の形態においては、ディスク製造識別情報DiscIDm及びディスク記録識別情報DiscIDmは、M系列符号を用いて暗号化したが、本発明はこれに限定されない。例えば、通常使用しない変調方式を使ったり、通常使用しないエリアに書いたり、すかし(watermark)のように希薄化した情報を光ディスク全体など広い範囲に分散させて書くことによって、上記識別情報に対するアクセスを阻止することができる。

【0122】

【発明の効果】上述のように、本発明においては、製造者により予め記録媒体に記録された第1の識別情報と、記録装置により記録媒体に記録された第2の識別情報との両方に基づいて、情報の暗号化／復号を行っている。従って、本発明によると、記録媒体に記録された情報について従来よりも確実に不正コピーを抑制することができる。

【0123】すなわち、たとえ製造業者が同一の第1の識別情報を記録した記録媒体を複数製造しても、記録装置がそれぞれ別個の第2の識別情報を記録するので、識別情報全体として別個のものとなり、この識別情報にアクセスされない限り不正コピーを防ぐことが可能となる。

【0124】また、たとえ記録装置が持つ第2の識別情報の記録方法を不正者が盗んだとしても、それだけでは製造業者が記録した第1の識別情報にアクセスすることはできず、この場合も不正コピーを防ぐことが可能となる。

【図面の簡単な説明】

【図1】本発明を適用した光ディスク記録再生装置の一実施の形態の構成を示すブロック図である。

【図2】特願平10-025310号明細書に記載されている記録方法により光ディスクに記録されるデータを説明する図である。

【図3】光ディスクに記録されるデータを説明する図である。

【図4】暗号化部の内部の構成を示す図である。

【図5】復号部の内部の構成を示す図である。

【図6】DiscIDm書き込み装置の内部の構成を示す図である。

【図7】DiscIDm書き込み装置の動作を説明するフローチャートである。

【図8】の暗号化部の動作を説明するフローチャートである。

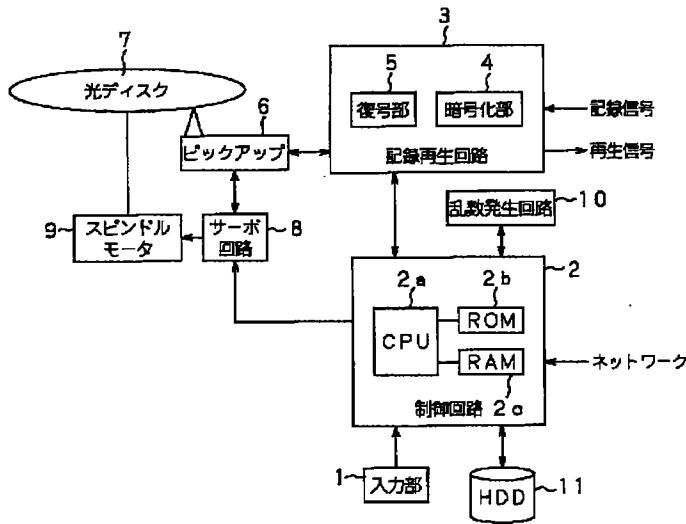
【図9】の復号部の動作を説明するフローチャートである。

【符号の説明】

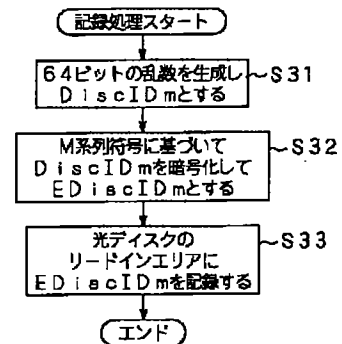
1 入力部, 2 制御回路, 3 記録再生回路, 4 暗号化部, 5 復号部, 6 ピックアップ, 7 光ディスク, 8 サーボ回路, 9 スピンドルモータ, 10 乱数発生回路, 21 DiscID暗号化復号回路, 22 M系

列符号発生回路, 23 Kem発生モジュール, 24 Kmメモリ, 25 hash関数回路, 26 Kd暗号化復号回路, 27 Ks暗号化回路, 28 コンテンツデータ暗号化回路, 51 EDiscID復号回路, 52 M系列符号発生回路, 53 Kem発生モジュール, 54 Kmメモリ, 55 hash関数回路, 56 EKd復号回路, 57 EKs復号回路, 58 コンテンツデータ復号回路

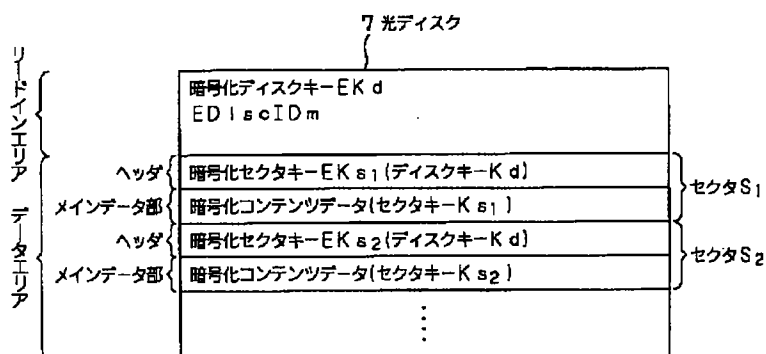
【図1】



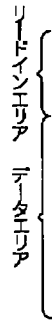
【図7】



【図2】



7 光ディスク



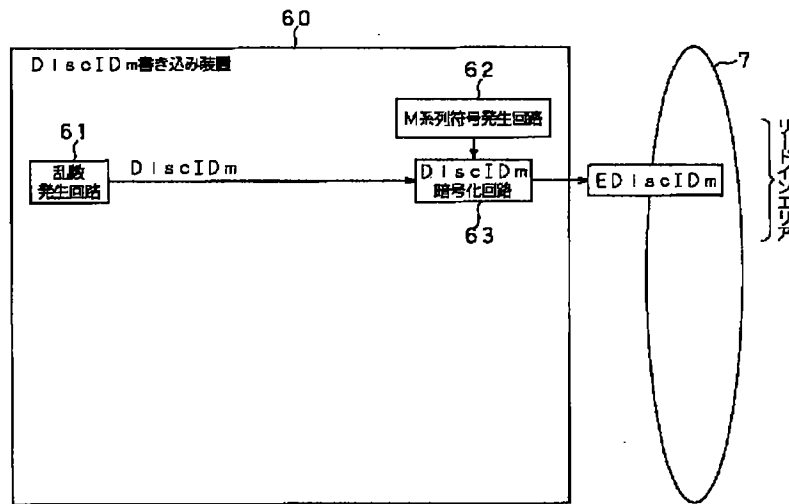
【図4】



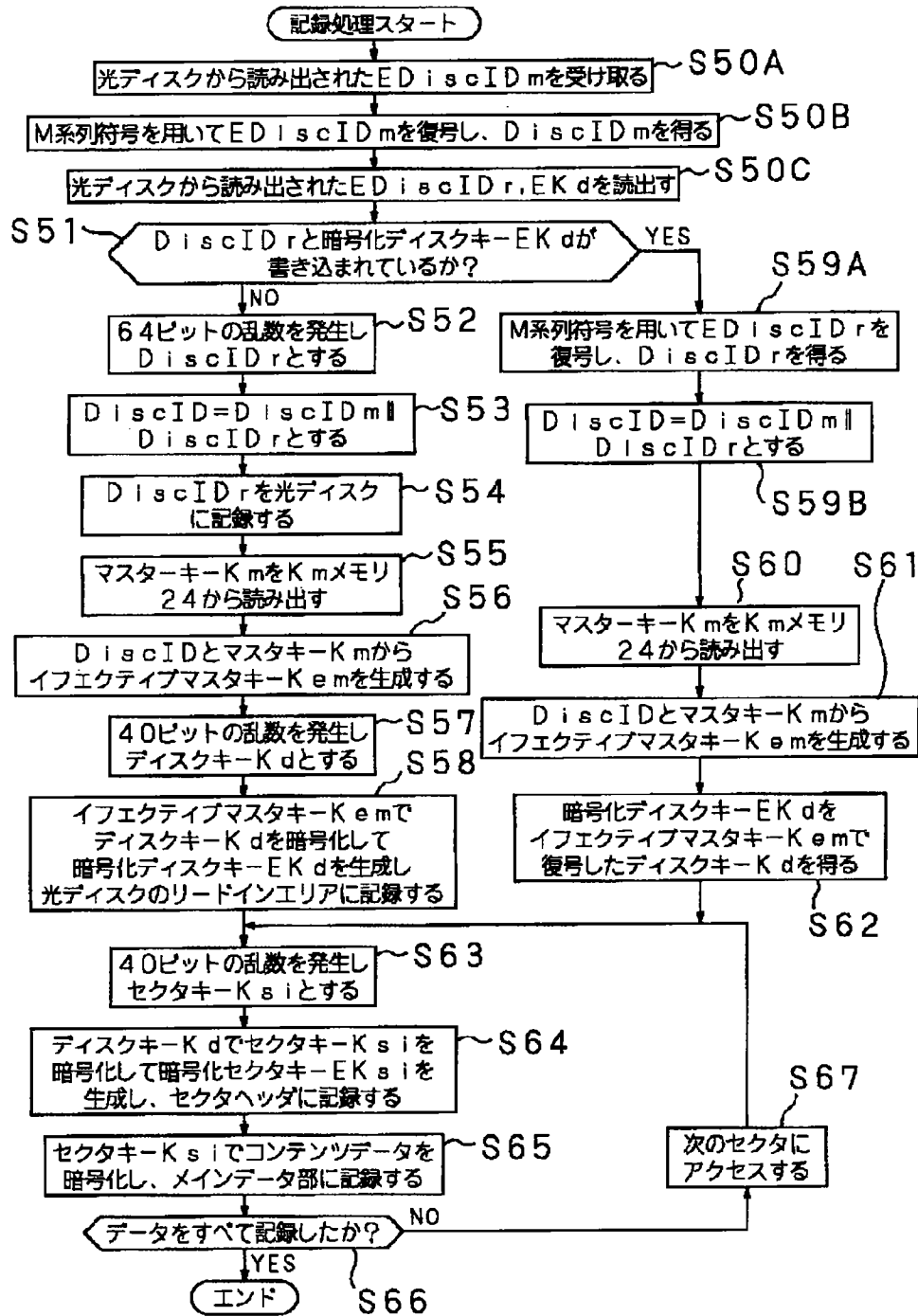
【図 5】



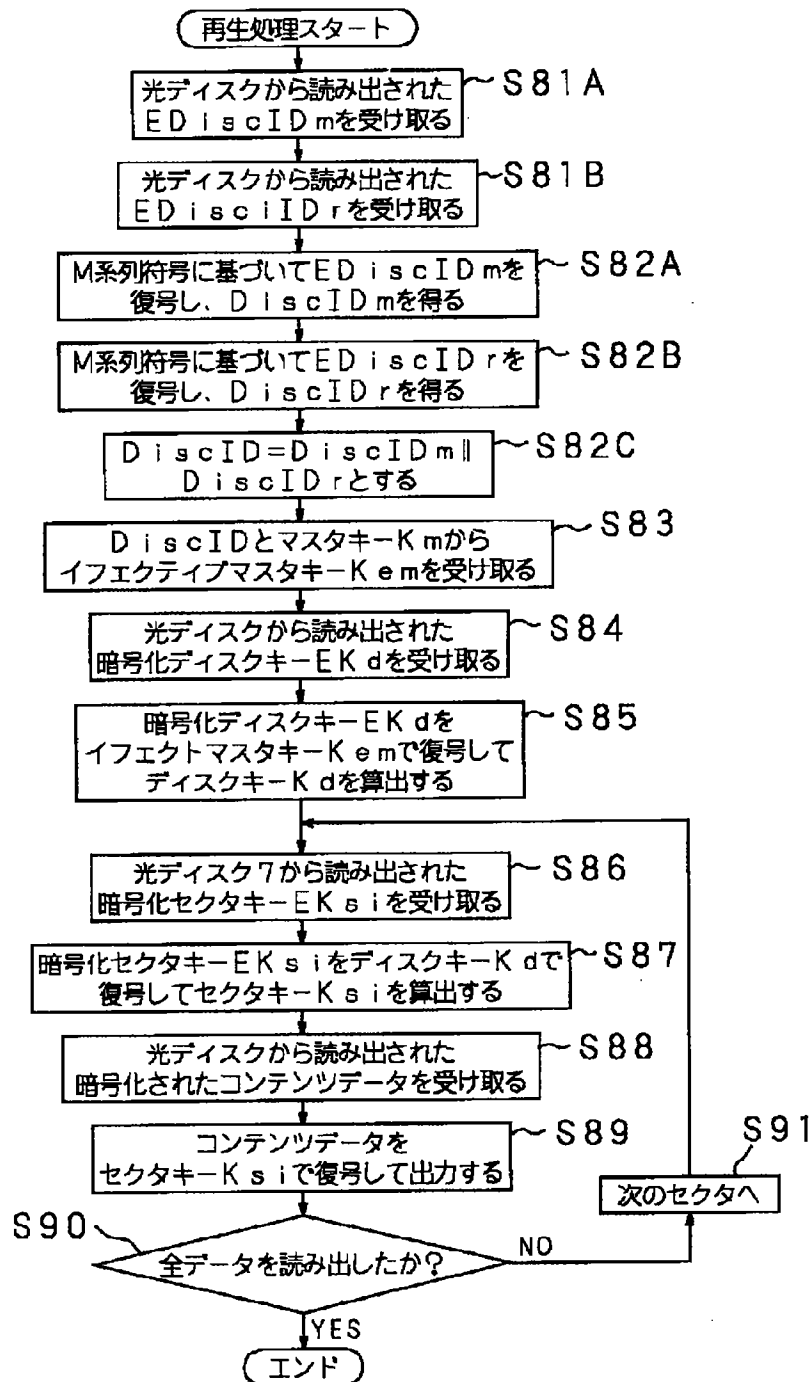
【図6】



【図8】



【図9】



フロントページの続き

Fターム(参考) 5D044 AB05 AB07 BC02 CC01 CC04
 DE48 DE52 EF05 FG18 GK12
 GK17 HL08
 5J104 AA12 AA16 AA34 EA06 EA15
 EA19 EA20 EA26 JA13 NA02
 NA12 NA32 NA37 NA38 PA14